IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

BLUE FLAME MEDICAL LLC ***Plaintiff,*** **v.** **CHAIN BRIDGE BANK, N.A., JOHN J. BROUGH, and DAVID M. EVINGER,** ***Defendants.***	**Civil Action No. 1:20-cv-00658** **The Honorable Leonie Brinkema**
CHAIN BRIDGE BANK, N.A. ***Third-Party Plaintiff*,** **v.** **JPMORGAN CHASE BANK, N.A.** ***Third-Party Defendant.***	

PLAINTIFF BLUE FLAME MEDICAL LLC'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

PRELIMINARY STATEMENT

The undisputed material facts establish liability with respect to the Regulation J/UCC Article 4A claims (Counts I and II) against Chain Bridge Bank, N.A. ("Chain Bridge") and the tortious interference claims (Counts IV and V) against Chain Bridge and its senior executives, John Brough and David Evinger (together with Chain Bridge, "Defendants"). Chain Bridge accepted the $456,888,600 Fedwire transfer at issue and could not cancel that wire transfer after its acceptance as a matter of law. Not one of the specific and narrow bases for cancellation of a Fedwire transfer under UCC Article 4A applies to the facts here. Far from demonstrating that the wire transfer was unauthorized or a mistake, the undisputed facts demonstrate that the State of California approved the payment to Blue Flame Medical LLC ("Blue Flame") to procure desperately-needed personal protective equipment ("PPE") to combat the COVID-19 pandemic. Defendants were fully aware of all of these facts.

Defendants knew that the wire transfer had been completed and could not be canceled. Nevertheless, Chain Bridge returned the funds to California's bank, JPMorgan Chase, N.A. ("JPMC"), without notifying or obtaining consent from Blue Flame. They accomplished this illegal transfer through a burst of direct communications with California and JPMC, baselessly casting doubt on their own customer's credibility even though Blue Flame had advised Chain Bridge of the incoming wire transfer, its purpose, and the specific amount the day before. The return of the wire transfer solved Chain Bridge's concerns about the effect that such a large deposit would have on its balance sheet, but it did so in violation of law and at the expense of its customer's interests and the contract between Blue Flame and California to supply life-saving PPE.

As set forth below, Chain Bridge's actions in returning the wire transfer violated Federal Reserve Board Regulation J, which incorporates Article 4A of the UCC and governs the handling of wire transfers. Chain Bridge violated Section 4A-404 and is liable to Blue Flame for damages

because it accepted but then withdrew or refused payment of the wire transfer amount to Blue Flame. Second, Chain Bridge violated Section 4A-204 because it sent an unauthorized transfer from Blue Flame's account in order to return the funds to JPMC and the State of California, and is therefore liable to Blue Flame for the misappropriated funds. Finally, all Defendants are liable to Blue Flame for tortious interference with contract and business expectancy because the undisputed facts show that they intentionally interfered with Blue Flame's relationship and contract with the State of California and that their actions were contrary to banking law and industry practice.

STATEMENT OF UNDISPUTED MATERIAL FACTS

A. Gula and Thomas Form Blue Flame.

Blue Flame was founded by Mike Gula and John Thomas in March 2020 to provide urgently needed PPE at fair prices to state and local governments, first responders, and healthcare providers to battle the COVID-19 pandemic. Ex. 1, 24:7-15; Ex. 2, 50:2-51:19.[1] Gula and Thomas previously worked as political consultants but decided in early 2020 to transition to a new career. *See* Ex. 2, 50:2-51:19. In February 2020, Gula and Thomas founded Blue Flame Strategies, a consulting company that leveraged their relationships with suppliers and distributors of PPE and their knowledge of governmental operations and contacts to help connect distributors to those in need of PPE. Ex. 1, 41:2-14. Beginning in March 2020, Gula and Thomas recognized they had opportunities to distribute PPE directly to customers in light of their supplier relationships. Ex. 2, 56:9-57:14. Blue Flame formally incorporated on March 23, 2020 for that purpose, though Thomas

[1] Citations to "Ex. [Number]" refer to the corresponding exhibit attached to the Affirmation of Peter White in Support of Motion for Partial Summary Judgment, filed contemporaneously with this Memorandum.

and Gula discussed potential PPE sales by Blue Flame prior to that date, including with California. SUF[2] ¶ 9; Ex. 2, 99:11-21; Ex. 3, 121:2-122:2.

B. Blue Flame Negotiates with California to Supply 100 Million N95 Masks.

On March 20 and 21, 2020, Thomas began discussing Blue Flame's ability to deliver N95 masks and other PPE with California officials, including State Controller Betty Yee. SUF ¶ 6; Ex. 4, BFM000200119. Thomas ultimately was referred to Michael Wong, a Contracts Administrator tasked with PPE procurement at the California Department of General Services ("DGS"), the California agency responsible for negotiating PPE purchases and vetting potential suppliers. Ex. 5, BFM000200135; Ex. 6, 15:19-17:5.

On March 22, 2020, Wong began discussing a purchase of N95 masks and COVID test kits with Thomas. *See id.*; SUF ¶ 7. Over the next two days, Wong and Thomas discussed how Blue Flame's suppliers, like others at the time, were requiring prepayment to secure production due to unprecedented demand, and that DGS should move quickly if it wished to secure the products. Ex. 5, BFM000200135. At Wong's request, Thomas provided inventory and product specification sheets for items that Blue Flame could deliver. *Id.*, BFM000200136-38; Ex. 7, BFM000066185-86; Ex. 8, BFM000116042-100; Ex. 9, BFM000116128 & 34. California's Department of Public Health used those specification sheets to identify four models of N95 masks that met its requirements. Ex. 10, DGS5563-64.

On the afternoon of March 24, Wong asked what volume of those four models could ship immediately, and told Thomas to "shoot for 100M." Ex. 5, BFM000200138-139. Thomas inquired with Blue Flame's suppliers—including Great Health Companion ("GHC") and Suuchi Inc. ("Suuchi"). Both confirmed they could supply the masks that California had specified (Ex. 20,

[2] "SUF" refers to the joint Stipulation of Uncontested Facts, Dkt. No. 96.

BFM000013611; Ex. 72, BFM000116661), and Thomas responded that Blue Flame could deliver at least 63 million units within 30 days, but that he needed to confirm exact capacities, (*id.*, BFM000200139; Ex. 11, BFM000110970-71). Wong confirmed that California could pay 75% of the total order cost up front and, after being told the price per mask was $3.80-$4.80 per mask plus shipping, handling, and tax, Wong asked if California "could execute on this today[.]" Ex. 11, BFM000110967-69. Wong then asked Thomas for an invoice for 100 million N95 masks. *Id.*, BFM000110967.

On March 25, 2020, DGS formally agreed to purchase 100 million N95 masks at $4.76 each, plus tax and estimated shipping costs, for a total of $609,161,000. *See* SUF ¶ 8. Thomas provided the invoice that Wong requested. Ex. 12, BFM000111121-22. California used that invoice internally to prepare a wire transfer to Blue Flame of 75% of the invoiced amount—$456,888,600—as prepayment to enable Blue Flame to secure the allocation of N95 masks from its suppliers (the "Wire Transfer"). SUF ¶ 8; Ex. 13, DGS0212-25.[3] Wong then confirmed with Thomas that California would send the wire the morning of March 26. Ex. 14, BFM000111148. Thomas and Gula also received confirmation on March 25 from the Chief Executive Officer of Blue Flame's primary supplier for California's order, GHC, that his company could deliver 100 million masks of the four specified models to California within 30 days if prepayment was made to lock down production lines with manufacturers. Ex. 15, BFM000212725-26; Ex. 2, 201:3-202:5. At the request of the Director of DGS, Thomas provided a "list of rough delivery timelines and manufacturers" for the shipment of the masks to California the night of March 25. Ex. 16, BFM000129959-60; Ex. 2, 220:6-221:6. That list indicated that Blue Flame's suppliers, Suuchi

[3] Wong also prepared an internal DGS purchase order reflecting similar information and listing a delivery date of April 3, 2020 for the first shipment of masks. Ex. 17; Ex. 18, 108:12-109:2.

and GHC, would attempt to deliver all 100 million masks within 30 days, but Blue Flame and California officials understood the goal was to deliver the masks as soon as possible. Ex. 2, 220:6-221:19; Ex. 6, 98:2-99:21. By the next morning, Blue Flame had written confirmation from and reseller agreements in place with both Suuchi and GHC to supply the masks California had ordered. Ex. 19, BFM000116424-25; Ex. 20, BFM000013610-11; Ex. 21, BFM000072920-31; Ex. 22, BFM000001541-51.

C. **Blue Flame Opens the Account and Notifies Defendants of the Transaction.**

Blue Flame opened a business checking account at Chain Bridge on the morning of March 25, selecting Chain Bridge as its bank because Gula had used Chain Bridge for his personal and business banking for over a decade. *See* Ex. 1, 141:15-142:8; SUF ¶ 10; Ex. 23, CBB00000555-56. That morning, Gula corresponded with Maria Cole, the relationship manager for Blue Flame's account, regarding Blue Flame's need for wire instructions to receive funds from California, its need to be immediately notified once the wire was received, and its need to send and receive payments the same day. *See* Ex. 24, CBB00001781-82; Ex. 25, CBB00001514. Cole then emailed Gula wiring instructions and a verification letter for the account. SUF ¶ 10; Ex. 24, CBB00001781 & 83-84.

That afternoon, Gula called Chain Bridge to discuss the anticipated incoming Wire Transfer from California. SUF ¶ 11; *see also* Ex. 1, 100:10-104:3; Ex. 2, 187:1-190:19. Gula discussed the wire and amount at 3:27 PM ET with Heather Schoeppe, the Bank's Senior Vice President and Branch Manager, and asked to be notified as soon as the funds were received. SUF ¶ 11; Ex. 26, 137:17-138:1. At 4:12 PM ET, Gula also confirmed the size of the wire with Cole via email. SUF ¶ 12; Ex. 27, CBB00003573; Ex. 1, 172:11-174:16. On a subsequent call with Schoeppe minutes later, Gula explained that California was purchasing 100 million N95 masks from Blue Flame, that Blue Flame would be purchasing the masks from its suppliers in China as

they were manufactured, and that Blue Flame anticipated keeping its profit in the account. SUF ¶ 13; Ex. 26, 155:4-157:7; Ex. 28 (audio); Ex. 29, CBB000000854-56. In response, Schoeppe congratulated Gula on the transaction. Ex. 26, 156:3-4; Ex. 28 (audio).

Immediately after hanging up with Gula, Schoeppe told others at Chain Bridge about her discussions with Gula, including Brough. Ex. 29, CBB000000854-56. Minutes later, Schoeppe spoke to the Bank's Chief Financial Officer, Joanna Williamson, who said the size of the wire "would have a really big impact on [Chain Bridge's] capital ratios"—which were to be calculated as of March 31—and discussed using an Insured Cash Sweep ("ICS") account to keep the funds off the Bank's balance sheet to limit those impacts. *See* Ex. 30 (audio), 1:56-2:30; Ex. 31, 20:16-21:13. Schoeppe then spoke to Brough and Evinger; Evinger confirmed that he knew Gula and Brough said that if Chain Bridge received the wire, it "can't hold that money on our balance sheet" and would need to use an ICS account or similar program to keep the funds off of the Bank's balance sheet. Ex. 32 (audio), 2:52-3:20. Brough remarked that Blue Flame would "make $100 million off selling the masks or something stupid like that," wondered if "someone's penetrated state coffers," and agreed to notify the Bank's Chairman and call Gula to discuss the transaction with him further. *Id.*, 9:25-9:45, 11:20-11:30, 12:37-12:43, 13:17-13:36.

Brough and Evinger then called Gula. SUF ¶ 14. During that approximately 19 minute call, Gula explained the relevant details concerning the California transaction, Blue Flame's business and Gula's transition away from politics, Blue Flame's immediate needs, and Blue Flame's expected receipt of the wire. *See* Ex. 1, 193:5-196:1. Among other things, they discussed that:

- Blue Flame would be receiving a wire transfer for approximately $450 million from the State of California (Ex. 33, 191:15-20; Ex. 34, CBB00004445; Ex. 35, 135:4-140:17; Ex. 84, BFM000137279-80);
- The Wire Transfer was California's down payment for the purchase of 100 million N95 masks from Blue Flame (Ex. 35, 131:18-132:5; Ex. 33, 190:14-18; Ex. 1,

180:20-181:4; Ex. 34, CBB00004445; Ex. 36, CBB00004442);

- Blue Flame would use portions of California's down payment to send outgoing wire transfers to domestic bank accounts for its suppliers (Ex. 35, 133:20-134:2, 147:22-149:11; Ex. 33, 192:21-194:5; Ex. 84, BFM000137279-80); and

- The N95 masks for California would be manufactured in China and GHC would serve as one of the suppliers for California's order (Ex. 35, 133:10-134:8; Ex. 33, 191:21-192:11; Ex. 1, 180:20-181:4; Ex. 34, CBB00004445; Ex. 36, CBB00004442; Ex. 84 BFM000137279-80).

During that discussion, Brough and Evinger indicated the wire's size would pose operational challenges for the Bank, but that the Bank was able to handle it. *See* Ex. 35, 244:8-245:5; Ex. 84 BFM000137279-80. Gula told Brough and Evinger that he would provide any additional information concerning the transaction that Chain Bridge required. Ex. 1, 193:5-196:1; Ex. 84 BFM000137279-80.

That evening, Evinger emailed Gula to ask "[j]ust one question. Did you send any money to China or others as a 'fee' for these transactions?" Ex. 37, BFM000013445. Gula immediately responded, "[N]o, we have not sent the money to China but when we do this is where we are sending it. [P]lease let me know if you have any questions." Gula attached wire instructions for GHC identifying the U.S. bank account of its California-based affiliate. *Id.*, BFM000013445 & 48. Shortly thereafter, Gula forwarded to Evinger and Brough a text message from Wong to Thomas confirming that California would be paying Blue Flame the next morning. Ex. 38, CBB00002699-700.

Defendants did not indicate to Blue Flame at any point before, during, or after those discussions that Blue Flame had provided insufficient information, that Chain Bridge might not be willing or able to serve as Blue Flame's bank, that a wire of that size would cause balance sheet and capital problems for the bank, that it might not accept or would return the funds to California, or that Blue Flame would not be able to make the immediate outgoing wire transfers to its suppliers

that Gula had previewed. *See* Ex. 1, 193:5-196:1. Nevertheless, Brough emailed others at the Bank to report on his and Evinger's discussions with Gula, noting that while Gula was "very confident about the transactions," Brough and Evinger were "very skeptical" and that the Bank's Chairman "also thinks it is a scam." Ex. 39, CBB00000761. Brough closed his email by saying, "[i]n the event we do receive the cash, there is no way we can hold it on our balance sheet," and requested that Bank personnel prepare to "move the money off balance sheet" using the ICS program. *Id*.

D. Chain Bridge Accepts the Wire Transfer and Credits Blue Flame's Account.

The morning of March 26, Blue Flame remained in contact with Defendants to confirm details of the Wire Transfer. At 11:01 AM ET, Thomas called the Bank and spoke with Cole, explaining that he needed to confirm receipt of the wire with the suppliers of the masks "once I've got the funds" and that the wire from California was critical because "this is the initial wire that gets us so we can fill those other orders." Ex. 40 (audio), 2:37-2:49, 3:52-4:47.

At 11:21 AM ET, California's State Treasurer's Office ("STO") sent the wire, contacted JPMC to "ensure it is completed quickly," and verified the details, including the amount and beneficiary information. SUF ¶ 15; Ex. 41, JPMC-0000028; Ex. 42, 35:9-36:20, 39:3-40:5, 121:21-123:3. Within minutes, and after JPMC's internal monitoring system flagged the outgoing wire, JPMC confirmed that it had been authorized by the State Treasurer's Office, and Tim Coffey, a member of JPMC's internal fraud monitoring team, approved the outgoing wire. Ex. 43, JPMC-00000084-88; Ex. 44, 42:9-48:9, 48:15-49:20.

At 11:55 AM ET, the Wire Transfer was processed through Fedwire. SUF ¶ 16. All details on the wire transfer notice—including the Originator (DGS), Beneficiary (Blue Flame), and amount ($456,888,000)—matched the information Gula provided Defendants the day before. Ex. 45, CBB00002779; Ex. 35, 122:1-15; Ex. 33, 103:16-104:8. The incoming wire was flagged by Chain Bridge's internal monitoring system and was manually approved by Rick Claburn in the

bank's Operations department. Ex. 46, CBB00002649; Ex. 47, 100:17-101:22. Minutes later, Claburn emailed bank personnel to notify them that "[t]he wire has been received and credited to the client's account." Ex. 59, CBB00000664; *see also,* Ex. 48; CBB00002673.

At 11:59 AM ET, Gula received an "Incoming Wire Confirmation" email containing a link to a secure message reflecting Chain Bridge's acceptance of the Wire Transfer. Ex. 50, CBB00001938-39; SUF ¶ 17. At the same time, Thomas called Cole and explained that Gula had received the notification email but was having difficulty opening the secure message and needed to confirm the amount; Cole responded that she would check and call back. Ex. 52 (audio). At approximately 12:00 PM ET, Gula was able to access Blue Flame's account through the Bank's web portal and confirmed the funds were displayed in the account. Ex. 1, 221:2-17; *see also* Ex. 2, 226:6-17.

At 12:02 PM ET, Cole called Thomas back to confirm the amount of the wire that Chain Bridge had accepted. Ex. 53, CBB00004437; Ex. 2, 225:4-227:1. They then discussed Blue Flame's need to send an outgoing wire to Suuchi, one of its suppliers for the masks. *See* Ex. 53, CBB00004437; *see also* Ex. 2, 190:7-19. Cole confirmed that Chain Bridge could manually process the wire, and Thomas agreed to send the wire instruction details to Cole. *Id.* at 225:4-227:1. At 12:10 PM ET, Cole emailed Thomas a form for Blue Flame's requested outgoing wire transfer. Ex. 54, CBB00001725. At 12:12 PM ET, Cole informed the Bank's Operations staff that Blue Flame "will wire out today 2 wires totaling $22,680,000.00" and asked to confirm that the "[f]unds are available." Ex. 55, CBB000000971. At 12:14 PM ET, Blue Flame's counsel emailed Cole at Thomas's request to provide wire instructions for the wire to Suuchi. Ex. 56, CBB00001385. Thomas then responded to confirm Blue Flame's authorization of the instructions and to request that the wire be prepared "asap[.]" Ex. 57, BFM000116678.

E. Defendants Contact California and Cast Doubt Regarding Blue Flame.

Simultaneous with Cole and Thomas's discussion about the outgoing wire transfer, at 12:02 PM ET, Schoeppe emailed Brough, Evinger, and others, stating "[w]ire has been received" with a screenshot from Chain Bridge's software system showing the "Credit" of $456,888,600 affecting the "Current Balance" in Blue Flame's checking account. Ex. 48, CBB00002673. In response, Brough forwarded Schoeppe's email to the Bank's Chairman, stating, "[u]nbelievable. We are going to try to contact the sender." Ex. 58, CBB00002731-32. A few minutes later, the Bank's Chairman responded to Evinger, directing him to "put the money in ICS as soon as you determine this money is legitimate" (*id.*); however, the ICS program had a maximum limit of less than one-third the size of the Wire Transfer, raising concerns "around how long these funds would be on deposit[.]" Ex. 59, CBB00000662-63. At 12:07 PM ET, Evinger directed that Chain Bridge place a "hold" on the funds in Blue Flame's account (SUF ¶ 18), though the requested hold was not applied to Blue Flame's account until 12:25 PM ET. Ex. 60, CBB00004468. At the same time, Brough directed the Bank: "Do not contact the client about this wire." Ex. 61, CBB000000748. Brough then updated the Bank's Chairman, stating: "We are attempting to contact [DGS]." Ex. 58, CBB00002731.

Between 12:15 PM and 12:21 PM ET, Evinger placed calls to three California state offices, including DGS, requesting that someone call him back to discuss the Wire Transfer. Ex. 62, CBB00004333-35. Shortly thereafter, Coffey contacted Chain Bridge to inform Evinger that JPMC was conducting an investigation of the Wire Transfer; Evinger responded that Chain Bridge had already placed a hold on the funds and falsely stated that Chain Bridge had not credited Blue Flame's account. *Id.*; Ex. 63, 64:19-66:7; Ex. 44, 63:15-64:2, 71:22-72:8, 138:21-139:14. That was significant to JPMC since it believed that whether the funds had been credited impacted whether they could be returned without the beneficiary's authorization. Ex. 44, 38:14-40:2. At 12:44 PM

ET, Brough and Evinger then spoke to Rakesh Korpal of JPMC regarding the Wire Transfer and JPMC's investigation. Ex. 64 (audio).[4]

At 12:50 PM ET, while Brough and Evinger were speaking to Korpal, DGS's Chief Accounting Officer, Fee Chang, returned Evinger's call and left a voicemail confirming the legitimacy and exact amount of California's wire to Blue Flame. Ex. 65 (audio); Ex. 33, 246:17-248:1; Ex. 35, 276:9-287:17. At 12:55 PM ET, Brough and Evinger spoke to Chang, who again confirmed the legitimacy of the Wire Transfer. In response, Brough and Evinger asked to speak to someone in the STO. Ex. 51 (audio); Ex. 62, CBB00004333-35. Shortly thereafter, Chang contacted Natalie Gonzales of the STO, stating that Evinger "requested to speak to someone in the [STO] right away to verify the wire amount is legitimate." Ex. 66, DGS4006.

At 1:19 PM ET, Gonzales and another STO official called Evinger and Brough. *See* Ex. 62, CBB00004333-35. During that call, the STO officials confirmed the Wire Transfer was authorized, that Blue Flame was the intended beneficiary, and the payment was being made for the purchase of N95 masks. Ex. 35, 144:14-145:11, 282:19-283:8; Ex. 33, 225:19-226:17, 249:22-251:19. Rather than verify the amount or inquire about the transaction, Brough and Evinger told the STO officials Blue Flame's account had been opened the day before by lobbyists and offered to return California's payment. Ex. 42, 127:4-130:5, 132:6-18; Ex. 67, CBB00004466. In response, the STO officials asked if the funds had been credited to Blue Flame's account, and Evinger said—again, falsely—that they had not. Ex. 42, 83:7-84:12, 91:1-92:5, 131:9-16.

[4] Brough recorded a portion of this conversation with Korpal and other conversations concerning the Wire Transfer manually using his smartphone without informing or obtaining consent from the other parties to the conversation, something he had never done before in his career. *See* Ex. 35, 128:19-130:22, 263:10-265:8. Evidently, he chose not to record the discussion with Gula on March 25 or his and Evinger's discussion with the STO on March 26, discussed below.

F. Defendants Cause JPMC to Request a Recall of the Funds and Refuse to Discuss the Wire Transfer with Blue Flame.

At 1:34 PM ET, Korpal called back Evinger and Brough and said that the California representatives JPMC had spoken to were "a bit unsure." Ex. 68 (audio), 0:00-0:03. In response, Evinger asked if JPMC could "issue a recall for the wire, so that while you intervene in this, you have the funds and feel more comfortable?" *Id.*, 0:03-0:14. Korpal responded, "I feel comfortable that you're holding the money right now. I can issue a recall, but I don't think you or I want to get onto the front page of the *Wall St. Journal*, especially if this is a legitimate transaction." *Id.*, 0:15-0:28. After the call, based on Chain Bridge's request that JPMC recall the funds and his belief that Blue Flame's account had not been credited, Korpal directed Coffey to request Chain Bridge to return the funds. *See* Ex. 44, 38:14-40:9, 62:8-64:2, 79:14-19; *see also* Ex. 63, 154:18-157:12.

Brough and Evinger then discussed the recall with Bank Operations personnel and instructed them to return the funds to JPMC. Ex. 69 (audio), 0:00-0:42. Claudia Mojica-Guadron, a Chain Bridge Operations technician, asked whether JPMC would be providing an indemnity letter to Chain Bridge, explaining that "[n]ormally, you want to get that from the other bank just because, and in this case because we credited the customer's account." *Id.*, 1:17-1:25, 2:15-2:27. Brough responded "don't worry about it…it is what it is. [Evinger] and I have been working on this with both the State of California and JPMorgan, and this is what we have to do." *Id.*, 2:27-2:49. At 1:45 PM ET, JPMC sent the recall request via Fedwire that Defendants requested. Ex. 70, CBB00002651-52.

While Brough and Evinger were busy discussing the Wire Transfer with California officials and JPMC, Blue Flame repeatedly tried to contact Chain Bridge after Gula realized that he could no longer access Blue Flame's account through the Bank's web portal. *See* Ex. 62, CBB00004348-49; Ex. 1, 203:19-22, 206:15-210:20; Ex. 2, 228:7-229:2. Chain Bridge personnel

did not respond and refused to discuss the Wire Transfer as Brough had directed. *See* Ex. 61, CBB000000748. At 1:34 PM ET, Gula emailed Evinger and Brough, asking "can someone call me asap please?" Ex. 71, BFM000074101-02. At 1:56 PM ET, Brough finally responded to Gula: "We received official notice from the sending bank to return the wire. Please resolve directly with the state of California." *Id.*

G. Defendants Send the Funds Back to JPMC and Close Blue Flame's Account.

At 2:36 PM ET, while the Bank's Operations personnel were preparing to send the funds in Blue Flame's account back to California without its consent, Brough instructed Schoeppe to close Blue Flame's account and all other accounts recently opened by Gula and Thomas. Ex. 73, CBB00000816. At 2:40 PM ET, Chain Bridge's Director of Operations requested that the account remain open until the funds were returned. *Id.*, CBB00000815.

At approximately 2:59 PM ET, Chain Bridge processed a new payment order on Blue Flame's behalf, without its consent, to return the funds in its account to JPMC. *See* Ex. 74, CBB00002781; Ex. 75, CBB00002653-54; Ex. 1, 206:15-210:20. That payment order listed Blue Flame as the Originator, DGS as the Beneficiary, and referenced the recall notice that JPMC had sent at Chain Bridge's Request. *See* Ex. 74, CBB00002781; Ex. 75, CBB00002653-54.

H. California Does Not Move Forward with Blue Flame.

After Chain Bridge sent the funds back to California's bank, DGS's Deputy Director for Administration, Andrew Sturmfels, announced that DGS would no longer be moving forward with Blue Flame as a vendor. Ex. 76, SCO0221; Ex. 77, SCO0131-32. Blue Flame nevertheless attempted to engage with DGS representatives in an effort to find a path forward for the transaction, but those efforts were unsuccessful. *See, e.g.*, Ex. 2, 255:16-21.

STANDARD OF REVIEW

Summary judgment is proper "if the movant shows that there is no genuine dispute as to

any material fact and the movant is entitled to judgment as a matter of law." Fed.R.Civ.P. 56(a). "Once the movant files for summary judgment and provides evidentiary support for the motion…, 'the nonmoving party must come forward with specific facts showing that there is a *genuine issue for trial*.'" *Integrated Direct Mktg., LLC v. May*, 129 F. Supp. 3d 336, 344 (E.D. Va. 2015) (emphasis in original) (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986)).

ARGUMENT

I. CHAIN BRIDGE IS LIABLE TO BLUE FLAME UNDER SECTIONS 4A-404 AND 4A-204 OF THE UNIFORM COMMERCIAL CODE.

UCC Sections 4A-404(a) and 4A-204(a) are incorporated by Federal Reserve Board Regulation J and provide causes of action against a bank for violation of Section 4A-211, which narrowly and expressly defines when a wire transfer may be canceled after a bank's acceptance on behalf of its customer.[5] Section 4A-404(a) addresses nonpayment of the wired funds; Section 4A-204(a) addresses the return of the funds to the originator. Chain Bridge is liable for consequential damages in an amount to be proven at trial under Section 4A-404(a) because it accepted the payment order JPMC sent on behalf of California but ultimately prevented Blue Flame from accessing the funds despite the impossibility of cancellation. Chain Bridge is liable under Section 4A-204(a) for a refund of the unauthorized payment order it sent on Blue Flame's behalf, but without its consent, in order to return the funds wired to Blue Flame by California.

A. Chain Bridge Violated § 4A-211 by Reversing the Wire Transfer Without Blue Flame's Consent.

Despite Defendants' unfounded assertion that Chain Bridge "canceled" the Wire Transfer

[5] *See* 12 C.F.R. pt. 210, subpt. B, app. B (2021). Citations below to the provisions of UCC Article 4A, as incorporated into Regulation J, are made directly to the relevant section of UCC Article 4A.

(*see, e.g.,* Ex. 35, 217:18-218:17), the undisputed evidence shows that Chain Bridge accepted the Wire Transfer and the law dictates that any attempted cancellation is not effective where, as here, the circumstances that permit cancellation do not exist.

Two independent undisputed facts prove that Chain Bridge accepted California's payment order for the account of Blue Flame: (1) the Wire Transfer was transmitted via the Fedwire Funds Service, and (2) Chain Bridge notified Blue Flame of its receipt of the order. *See, e.g.*, SUF ¶¶ 16-17; Statement of Undisputed Material Facts, *supra* ("SOF"), § D. Either fact establishes as a matter of law that Chain Bridge accepted the payment order. *See* UCC § 4A-209(b)(1); *id.* at (b)(2); UCC § 4A-403(a)(1); *see also* UCC § 4A-209(b), cmt. 6 (Am. Law Inst. 2017) ("Section 4A-209(b)(2) results in automatic acceptance of payment orders issued to a beneficiary's bank by means of Fedwire"). Once a beneficiary's bank accepts a payment order, the wire transfer is completed as a matter of law. UCC § 4A-104(a).

Section 4A-211(c)(2) provides the only means of canceling a payment order once it has been accepted by the beneficiary's bank. Even if the beneficiary's bank agrees to the sender's request to cancel the payment order, it provides:

> *cancellation or amendment is not effective* unless the [payment] order was issued in execution of an unauthorized payment order, or because of a mistake by a sender in the funds transfer which resulted in the issuance of a payment order (i) that is a duplicate of a payment order previously issued by the sender, (ii) that orders payment to a beneficiary not entitled to receive payment from the originator,[6] or (iii) that orders payment in an amount greater than the amount the beneficiary was entitled to receive from the originator.

UCC § 4A-211(c)(2) (emphasis added). Thus, where the sender has intentionally sent a payment

[6] The commentary to Section 4A-211 explains that this "not entitled to receive payment" language refers to a situation in which the payment order mistakenly orders payment to a beneficiary different from the one the originator intended to pay. UCC § 4A-203, cmt. 4, "*Case #3*," (Am. Law Inst. 2017). A mistake does not occur where payment is made to a beneficiary that the originator intended to pay, as is the case here.

order containing accurate payment and beneficiary information, as California did here, the payment order cannot be canceled once accepted by the beneficiary's bank. *See* UCC § 4A-211, cmt. 3 (Am. Law Inst. 2017) ("If the receiving bank has accepted the order, it is possible to cancel or amend but only if the requirements of subsection (c) are met."); *Bayerische Hypo-Und Vereinsbank Ag v. HSBC Bank USA, N.A.*, No. 602761/2009, 2015 WL 4455948, at *6 (N.Y. Sup. Ct. July 15, 2015) ("the beneficiary's bank is authorized to agree to cancellation after acceptance only in the circumstances that are specifically enumerated in [Section 4A-211(c)(2)].").

The undisputed facts known to both Chain Bridge and JPMC prior to the recall of the funds show that the payment order could not have been canceled without violating Regulation J. Defendants have admitted that every detail in the wire transfer message matched the information that Gula provided on March 25 (*see* Ex. 35, 122:1-15; Ex. 33, 103:16-104:8), and DGS and STO both confirmed that information to Brough and Evinger after the wire was received, (*see* SOF § E). JPMC also confirmed the amount and beneficiary information in California's payment order prior to releasing the wire to Chain Bridge. *See* SOF § D. Accordingly, cancellation of the wire was not possible as a matter of law pursuant to Section 4A-211.

That conclusion is consistent with the purpose of Section 4A-211 and Article 4A as a whole: to ensure finality of wire payments and promote certainty as to the rights and obligations of the parties to a wire transfer. *Banque Worms v. BankAmerica Int'l*, 77 N.Y.2d 362, 372 (1991) (citations omitted) ("Establishing finality in electronic fund wire transactions was considered a singularly important policy goal [by Article 4A's drafters]."). As the official comments explain:

> With respect to a payment order issued to the beneficiary's bank, acceptance is particularly important because it creates liability to pay the beneficiary [*see* § 4A-404], it defines when the originator pays its obligation to the beneficiary [*see* § 4A-406(a)], and it defines when any obligation for which the payment is made is discharged [*see* § 4A-406(b)]. *Since acceptance affects the rights of*

> *the originator and the beneficiary it is not appropriate to allow the beneficiary's bank to agree to cancellation or amendment except in unusual cases*. Except as provided in subsection (c)(2), cancellation or amendment after acceptance by the beneficiary's bank is not possible *unless all parties affected by the order agree*. Under subsection (c)(2), cancellation or amendment is possible only in the four cases stated."

UCC § 4A-211, cmt. 4 (Am. Law Inst. 2017) (emphases added). The sender of a wire needs to know when its payment obligation has been discharged, and the recipient needs to know when a payment is final so that it can use the funds, particularly where, as here, the originator's payment triggers the beneficiary's obligation to perform.[7] The Federal Reserve Board has stressed the importance of finality in Fedwire funds transfers in particular, stating: "The primary distinguishing characteristic of Fedwire is that payment orders are final and irrevocable to the receiver when made…. [T]he Board believes that Fedwire payment finality is vital to the continued integrity and efficiency of the payments system." Funds Transfers Through Fedwire, 55 Fed. Reg. 40791-01, 40800 (Oct. 5, 1990). Given the staggering volume of payments made via Fedwire—the average *daily* value of Fedwire transfers was more than $3.3 trillion in 2020—their finality is vital to the economy itself. *Fedwire® Funds Service - Annual Statistics*, The Federal Reserve, https://tinyurl.com/Fedwire-Annual-Stats.

The UCC comments to Section 4A-211 explain that these concerns with finality and certainty made it necessary to "severely limit[]" cancellation of completed funds transfers. *See* UCC § 4A-203, cmts. 4, 8 (Am. Law Inst. 2017); *Bayerische*, 2015 WL 4455948, at *8 (N.Y. Sup. Ct. July 15, 2015) (quoting UCC § 4A-102, cmt. 1) ("The drafters of Article 4A…made the

[7] Article 4A's Reporter has noted: "[I]t is very important in commercial transactions to have finality of payment. There is an awful lot of money involved in these cases, and money which is paid out to beneficiaries usually is immediately sent somewhere else." Address by Professor Robert Jordan, Reporter for Article 4A, American Law Institute Meeting (May 19, 1989), *reprinted in* 66 A.L.I. Proc. 399, at 414 (1989).

'deliberate decision' to limit cancellation of accepted orders in order [to] promote finality and predictability…."). Thus, Section 4A-211(c)(2) is designed to permit cancellation only where it would not disrupt the contractual obligations of the originator and beneficiary.[8] Section 4A-211 does not invite banks to exercise their own discretion as to whether cancellation is desirable.

Here, Chain Bridge attempted to cancel the payment order and then returned the funds despite having actual knowledge that none of the circumstances permitting cancellation was present, and without seeking the consent of the beneficiary, Blue Flame. Chain Bridge did so knowing that depriving Blue Flame of the funds to secure the masks from its suppliers would make it impossible for Blue Flame to perform its contract with California (*see* SOF § C), and knew or should have known that its actions would prompt California to renege on the contract. The reversal of the Wire Transfer also had devastating downstream effects on Blue Flame, which Chain Bridge knew was relying on the proceeds of the California transaction to fund fulfillment of other orders (*see* Ex. 40 (audio), 2:37-2:49, 3:52-4:47), to say nothing of the devastating reputational consequences Blue Flame suffered as a result of reporting on California's aborted transaction. By reversing a completed wire transfer in violation of Section 4A-211(c)(2), Chain Bridge created exactly the scenario that Section 4A-211, and Article 4A as a whole, was designed to prevent.[9]

Section 4A-211 expressly contemplates that a beneficiary bank incurs liability to its

[8] The four narrow circumstances permitting cancellation under Section 4A-211(c)(2) are not exceptions to that proposition; rather, they are particular, unusual circumstances in which misconduct or error in issuing the payment order may prevent a discharge of the originator's obligation *despite* acceptance by the beneficiary's bank. In any event, none apply here.

[9] Chain Bridge was not restricted in its options after JPMC requested that it cancel the payment order. Section 4A-211(c) expressly allows a bank to reject such a cancellation request. UCC § 4A-211(c); *id.*, cmt. 5 (Am. Law Inst. 2017) (emphasis added) ("a receiving bank may agree to cancellation or amendment of the payment order under subsection (c) but is not required to do so *regardless of the circumstances*.").

customer for an impermissible cancellation. UCC § 4A-211(f) (Am. Law Inst. 2017) (providing for sender's indemnification of beneficiary's bank that agrees to cancel payment order); *id.*, cmt. 5 ("If the receiving bank has incurred liability as a result of its acceptance of the sender's order, there are substantial risks in agreeing to cancellation or amendment."); *see Bayerische*, 2015 WL 4455948, at *6 ("If the bank were to agree to reverse the transfer, it would do so at its peril – unless the beneficiary were also willing to consent."). Sections 4A-404 and 4A-204 provide the causes of action for a violation of Section 4A-211(c)(2). Each provides a remedy for a distinct harm suffered by a beneficiary whose bank wrongfully reverses a wire transfer: Section 4A-404's claim addresses the beneficiary bank's failure to pay the beneficiary; Section 4A-204's claim addresses the beneficiary bank's return of the funds to the originator.

B. Chain Bridge is Liable Under Section 4A-404(a) for Accepting the Payment Order and then Withdrawing or Refusing Payment to Blue Flame.

UCC Section 4A-404(a) obligates the beneficiary's bank "to pay the amount of [an accepted] payment order to the beneficiary of the order." That provision also provides a cause of action to a beneficiary whose bank fails to satisfy its payment obligation:

> If the bank [i] [accepts a payment order but] [ii] refuses to pay [iii] after demand by the beneficiary and [iv] receipt of notice of particular circumstances that will give rise to consequential damages as a result of nonpayment, the beneficiary may recover damages resulting from the refusal to pay to the extent the bank had notice of the damages, unless the bank proves that it did not pay because of a reasonable doubt concerning the right of the beneficiary to payment.

UCC § 4A-404(a). There is no genuine dispute that all of those elements are present here. Accordingly, Chain Bridge is liable for damages in an amount to be proven at trial.

1. Chain Bridge accepted JPMC's payment order.

There is no dispute that Chain Bridge accepted the payment order. *See* Section I.A, *supra*; SUF ¶¶ 16-17; SOF, § D.

2. Chain Bridge withdrew or refused payment to Blue Flame.

There is no dispute that Chain Bridge failed to satisfy its obligation to pay Blue Flame. Whether this failure was effected by withdrawal of the payment initially made to Blue Flame or by failing to make payment to Blue Flame altogether is irrelevant; either satisfies this element of Blue Flame's claim.

Whether the beneficiary's bank has made payment to the beneficiary on an accepted payment order is governed by UCC Section 4A-405. Chain Bridge initially did make payment to Blue Flame by crediting Blue Flame's account, notifying Blue Flame of the credit, notifying Blue Flame that the funds were available to make outgoing wire transfers, and beginning the process of issuing an outgoing wire transfer. *See* SOF § D.[10] Any of those actions is sufficient to show that "the beneficiary [was] notified of the right to withdraw the credit," which constitutes payment under Section 4A-405(a). UCC § 4A-405(a). But despite initially notifying Blue Flame that it could withdraw the credit, Chain Bridge ultimately prevented Blue Flame from accessing the funds, thereby violating its obligation to make payment to Blue Flame under Section 4A-404(a).

3. Blue Flame demanded payment after Chain Bridge accepted the payment order.

Blue Flame demanded payment several ways, including Thomas's communications with Cole after Chain Bridge notified Blue Flame that it had received the Wire Transfer. Thomas instructed Chain Bridge, both over the phone and via email, to immediately send an outgoing wire transfer to Suuchi, one of its suppliers of N95 masks for California's order. Cole initiated that process on behalf of Chain Bridge before she and other bank personnel were ordered to stand down by Brough. *See* SOF § D. Blue Flame called Chain Bridge repeatedly on March 26 to demand

[10] Despite that clear evidence, Defendants nevertheless insist that Chain Bridge did not deposit the funds from the Wire Transfer into Blue Flame's account or notify Blue Flame of the right to withdraw the funds. *See, e.g.,* Ex. 35, 76:4- 77:18; Ex. 33, 256:3-260:14. Defendants are wrong, but their position would nevertheless satisfy this element for liability under Section 404(a).

payment and issue the wire transfer to Suuchi, but due to Brough's order, Blue Flame's calls went unanswered. *See* SOF § F.

4. Blue Flame notified Chain Bridge of particular circumstances that would give rise to consequential damages as a result of nonpayment.

The commentary to Section 4A-404 clarifies the nature of the notice required to establish a beneficiary bank's liability for consequential damages: "the bank [must] have notice of the general type or nature of the damages that will be suffered as a result of the refusal to pay and their general magnitude. There is no requirement that the bank have notice of the exact or even the approximate amount of the damages, but if the amount of damages is extraordinary the bank is entitled to notice of that fact." UCC § 4A-404, cmt. 2 (Am. Law Inst. 2017).

There is no dispute that Blue Flame gave notice of the type and magnitude of its potential damages, including notice that Blue Flame's consequential damages would be extraordinary. That notice was provided by Gula to Brough and Evinger during their 19-minute phone call on March 25, the day before California sent the Wire Transfer. That discussion put Defendants on notice that Blue Flame would receive a wire of over $450 million from California to procure and deliver 100 million N95 masks and complete a transaction worth over $600 million. *See* SOF § C. In fact, prior to Gula's call with Brough and Evinger, he already had provided that information to Schoeppe, to whom Brough remarked Blue Flame would profit over $100 million. *See, e.g., id.*; Ex. 32 (audio), 9:25-9:45. Furthermore, the morning of the Wire Transfer, Thomas told Cole about Blue Flame's intent to use the proceeds of the California transaction as seed capital for additional PPE transactions. *See* SOF § D. By notifying Chain Bridge's CEO, President, and a Senior VP of the purpose and value of the Wire Transfer and the underlying transaction, Blue Flame provided "notice of the general type or nature of the damages…and their general magnitude."

5. Chain Bridge did not have reason to doubt Blue Flame's right to payment.

The commentary to Section 4A-404 is unequivocal that the "reasonable doubt" defense articulated in the statutory text does not apply where the beneficiary's bank refuses to make payment due to concerns that its customer is engaged in fraud. Specifically, it provides:

> The last clause of subsection (a) *does not apply to cases in which a funds transfer is being used to pay an obligation and a dispute arises between the originator and the beneficiary concerning whether the obligation is in fact owed*. For example, the originator may try to prevent payment to the beneficiary by the beneficiary's bank by *alleging that the beneficiary is not entitled to payment because of fraud against the originator* or a breach of contract relating to the obligation. The fraud or breach of contract claim of the originator may be grounds for recovery by the originator from the beneficiary after the beneficiary is paid, but *it does not affect the obligation of the beneficiary's bank to pay the beneficiary*. Unless the payment order has been cancelled pursuant to Section 4A-211(c), *there is no excuse for refusing to pay the beneficiary and, in a proper case, the refusal may result in consequential damages*…. Thus, the beneficiary's bank may safely ignore any instruction by the originator to withhold payment to the beneficiary.

UCC § 4A-404, cmt. 3 (Am. Law Inst. 2017) (emphases added). Thus, any argument by Defendants that their purported fraud concerns constitute "reasonable doubt" sufficient to extinguish liability under Section 4A-404(a) should be rejected. *See AG4 Holding, LLC v. Regency Title & Escrow Servs., Inc.*, 98 Va. Cir. 89 (2018) (stating that where funds are fraudulently misdirected into the account of another, the victims "no longer had the right to possession of the funds at the very instant [the beneficiary's bank] accepted the payment order, even if fraud was involved."); *Go-Best Assets Ltd. v. Citizens Bank of Mass.*, 972 N.E.2d 426, 433 n. 6 (Mass. 2012).

Any doubt concerning Blue Flame's right to payment was resolved by the confirmations Chain Bridge received from DGS, STO, and JPMC that California intended to pay Blue Flame. *See* SOF § E; *see also* Ex. 42, 91:1-92:5, 86:19-88:18; Ex. 44, 42:9-49:20; Ex. 35, 122:1-15, 144:14-145:11, 276:9-277:5, 143:10-144:2; Ex. 33, 217:11-16, 225:19-226:17, 249:22-251:19;

Ex. 65 (audio); Ex. 83, 168:1-170:14; *see supra* Section I.A.

C. Chain Bridge is Liable Under Section 4A-204(a) for Sending an Unauthorized Funds Transfer in Order to Return California's Money.

Section 4A-204(a) makes banks liable for unauthorized wire transfers sent from a customer's account. It provides:

> If a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under § 4A-202, or (ii) not enforceable, in whole or in part, against the customer under § 4A-203, the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund.

UCC § 4A-204(a). Thus, where a bank reverses a completed funds transfer in violation of Section 4A-211(c)(2) without its customer's consent, the bank sends a payment order that is not authorized by the beneficiary and thereby incurs liability under Section 4A-204(a).[11] *Cf. First Sec. Bank of New Mexico, N.A. v. Pan Am. Bank*, 215 F.3d 1147, 1152 (10th Cir. 2000) ("Article 4A was crafted with the express purpose of creating—in an age of increasing automation—inflexible rules of liability for wire transfer disputes."). In reversing a completed wire transfer, the beneficiary's bank takes funds belonging to the beneficiary[12] and sends them back to the originator, an act which

[11] Chain Bridge is the "receiving bank" with respect to Blue Flame's Section 4A-204 claim. Section 4A-204 addresses the relationship between the originator of a funds transfer and the originator's bank. With respect to the payment order sent by the originator to its bank to initiate a funds transfer, the originator is the "sender" and the originator's bank is the "receiving bank." UCC §§ 4A-103, 4A-104. A bank that reverses a funds transfer in violation of Section 4A-211 and without its customer's consent, then, acts as the "receiving bank" with respect to the payment order it creates to reverse the transfer.

[12] *First Place Bank v. Olympia Logistics & Servs.*, Inc., No. 11-13542, 2013 WL 1122559, at *5-6 (E.D. Mich. Mar. 18, 2013) (quoting *U.S. v. BCCI Holdings (Luxembourg), S.A.*, 980 F. Supp. 21, 27 (D.D.C.1997)) (acceptance by beneficiary's bank entitles beneficiary to wired funds); *Bayerische*, 2015 WL 4455948, at *5 (N.Y. Sup. Ct. July 15, 2015) ("Under Article 4-A, title to the funds at issue thus passed to [beneficiary] on acceptance of the payment order by its bank.").

necessarily threatens the underlying transaction by giving the originator the chance to renege on its agreement with the beneficiary. Section 4A-204(a)'s cause of action thus addresses harm to the beneficiary that Section 4A-404(a)'s cause of action does not.

The facts establishing Chain Bridge's liability under Section 4A-204(a) are undisputed. Chain Bridge unilaterally created and accepted an unauthorized payment order on behalf of Blue Flame as the "Originator" to return the funds to California's STO as the "Beneficiary." *See* SOF § G; Ex. 75, CBB00002653-54; Ex. 78, CBB00002534; Ex. 79, CBB00000791-92.[13] Chain Bridge accepted that payment order when it sent the order to JPMC. UCC §§ 4A-209(a) ("A receiving bank other than the beneficiary's bank accepts a payment order when it executes the order."), 4A-301(a) ("executes" means "issues"), 4A-103(c) ("issues" means "sends"); 4A-203, cmt. 1 (Am. Law Inst. 2017). Therefore, Chain Bridge "accept[ed] a payment order issued in the name of its customer as sender." *See* UCC § 4A-204(a).

There is no dispute that Chain Bridge did not seek, let alone obtain, Blue Flame's authorization to issue the payment order to JPMC. *See* Ex. 1, 206:15-210:20; Ex. 61, CBB00000748.[14] Accordingly, the payment order Chain Bridge sent to JPMC was "not authorized and not effective as the order of the customer under § 4A-202." *See* UCC § 4A-204(a). As a result, Chain Bridge is liable for sending an unauthorized payment order in the name of Blue Flame as sender, and Blue Flame is entitled to a refund in the amount of that payment order.

[13] There is no dispute that the Fedwire message Chain Bridge sent JPMC to reverse the Wire Transfer had all of the requisite characteristics of a "payment order" as that term is defined in UCC § 4A-103(a)(1). *See* Ex. 75, CBB00002653-54.

[14] Nor did Chain Bridge follow any "security procedure" that would make the payment order effective as Blue Flame's order absent its express authorization. *See* UCC § 4A-202(b).

D. The Bank Secrecy Act Does Not Insulate Chain Bridge from Liability for Unilaterally Returning a Completed Wire Transfer Without Authorization.

Defendants have insisted that notwithstanding the clear rules set forth in Section 4A-404(a) and Section 4A-204(a), their actions were nevertheless justified because they were motivated by a desire to ensure Chain Bridge's compliance with the Bank Secrecy Act ("BSA"). *See, e.g.*, Ex. 35, 208:21-222:11. That position is meritless and does not shield Chain Bridge from liability.

The BSA is a recordkeeping and reporting statute. Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)," https://tinyurl.com/OCC-BSA-page ("The Bank Secrecy Act...establishes program, recordkeeping and reporting requirements…."). It requires banks to monitor and report activity they deem suspicious so that law enforcement authorities can decide whether the activity requires governmental action. *Id.* ("U.S. banks play a key role in combating the financing of terrorism by identifying and reporting potentially suspicious activity as required under the BSA."). The BSA does *not* grant a bank authority to reverse a completed wire transfer, nor does it address when a wire transfer may be reversed. *See generally*, 31 U.S.C. §§ 5311 *et seq.* The BSA does not imbue banks with the powers of a court or law enforcement, nor does it provide an exception to or exemption from any provision of Article 4A.

There is no tension between the BSA's requirements and those of Section 4A-211.[15] *See* Ex. 49, 25-31; Ex. 83, 308:3-316:10. Nevertheless, Defendants have suggested that a

[15] In fact, the BSA's implementing regulations, found at 31 C.F.R. Chapter X (2021), were drafted with Article 4A in mind. *See Funds Transfers: Questions & Answers*, 1 FinCEN Advisory 3, at A35 (June 1996) ("The Treasury and the Board have attempted to conform the definitions of the rule as closely as possible to UCC 4A definitions to avoid confusion in the banking industry."). In addition, the federal government's official BSA/AML Manual refers to Article 4A's rules concerning the finality of Fedwire funds transfers: "Payment over Fedwire is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving bank's Federal Reserve Bank master account or sends notice to the receiving bank, whichever is earlier." Bank Secrecy Act/Anti-Money Laundering Examination Manual, Federal Financial Institutions Examination Council, at 208 (2014), https://bsaaml.ffiec.gov/manual.

straightforward interpretation of Section 4A-211(c) would prevent a beneficiary's bank from satisfying its obligations under the BSA. *See* Ex. 35, 217:11-16; Ex. 80, 60:5-65:7. That is not true, as the BSA's requirements do not permit a wire transfer cancellation that is barred by Section 4A-211.

Defendants' appeal to the BSA also overlooks that Chain Bridge had a third "option" in addition to paying the Wire Transfer or canceling it: the bank could have held the funds while completing its due diligence on Blue Flame's transaction with California. *See, e.g., Go-Best Assets Ltd. v. Citizens Bank of Mass.*, 972 N.E.2d 426, 433 n. 6 (Mass. 2012) ("[I]f [the beneficiary's bank] owed a duty of care, it could not have prevented the funds from being deposited in [the beneficiary's] account and instead would have had to take reasonable steps to prevent [the beneficiary] from misappropriating the Go–Best funds in [the beneficiary's] account, either by freezing the account or otherwise ensuring that the Go–Best funds were safeguarded.").[16] None of Defendants' witnesses have explained why Chain Bridge did not take that course. *See* Ex. 35, 222:12-19, 226:8-17. That silence is particularly conspicuous given that Chain Bridge had placed a hold on Blue Flame's account before agreeing to cancel the payment order. Ex. 60, CBB00004468. If BSA concerns truly were motivating Defendants' actions, they could have continued to hold the funds pursuant to the terms and conditions of its account agreement with Blue Flame. Ex. 81, CBB00002774-75 & 77. Defendants instead reversed the Wire Transfer because holding the funds would not resolve the balance sheet concerns they and other Chain Bridge officers repeatedly expressed on March 25 and 26. *See* SOF § C; Ex. 31, 175:25-176:19.

[16] The Massachusetts Supreme Court also noted that "[t]he intrusive nature of such steps and the interference with the account holder's access to funds deposited in his account is justified *only where the bank has actual knowledge* of an intended or apparent misappropriation." 972 N.E.2d 426, 433 n. 6 (emphasis added).

II. DEFENDANTS TORTIOUSLY INTERFERED WITH BLUE FLAME'S CONTRACT WITH CALIFORNIA AND BUSINESS EXPECTANCY.

Tortious interference requires four elements: "(1) the existence of a valid contractual relationship or business expectancy; (2) knowledge of the relationship or expectancy on the part of the interferor; (3) intentional interference inducing or causing a breach or termination of the relationship or expectancy; and (4) resultant damage[.]" *Chaves v. Johnson*, 335 S.E.2d 97, 102 (Va. 1985). An additional element, "improper means" is also required when the contract is terminable at will or for a claim of interference with a business expectancy. *Dunlap v. Cottman Transmission Sys., LLC*, 754 S.E.2d 313, 318 (Va. 2014). There can be no dispute that each of the above elements is present here and Plaintiff should be granted summary judgment as to the liability of all three Defendants on Count IV for Tortious Interference with Contract and Count V for Tortious Interference with Business Expectancy.

A. A Valid Contract and Business Expectancy Existed.

There is no dispute that a valid contract and business expectancy existed between Blue Flame and California. Blue Flame had a contract to deliver 100 million masks to the state of California for $609,161,000, with an initial down payment of $456,888,600, sent to Chain Bridge via Fedwire on March 26, 2020. *See* SUF ¶ 8; SOF § B; Ex. 12, BFM000111121-22; Ex. 13, DGS0212-25; Ex. 46, CBB00002649.

B. Defendants Knew of the Contractual Relationship and Business Expectancy Between Blue Flame and California.

Defendants were aware of the contractual relationship and business expectancy between Blue Flame and California. Both Brough and Evinger testified extensively as to their knowledge of the existence of the contract and prospective business relationship. *See, e.g.*, Ex. 33, 217:20 (Blue Flame "had made arrangements with California"); *id.*, 217:15-16 ("[California] said they were doing business with Blue Flame Medical"); Ex. 35, 132:1-4 ("[Gula] told us that Blue Flame

was entering into a contract to sell a hundred million masks to the State of California"). Defendants also were aware that the money to be received was intended to pay Blue Flame's suppliers in order to perform its contract with California. Ex. 35, 133:10-134:2. There is no dispute that Defendants knew of the existence of a contract between Blue Flame and California. *See Tazewell Oil Co. v. United Va. Bank*, 413 S.E.2d 611, 625 (Va. 1992) (finding president of defendant-bank's notes of conversations sufficient to establish knowledge of contract).

Defendants' communications with California and JPMC verified their understanding of the contract and business expectancy. Upon receiving the wire transfer, Defendants took the unusual step of reaching out to California to verify the wire transfer, the amount of the payment, and confirm its business relationship with Blue Flame. *See* SOF § E; Ex. 33, 247:15-248:1. That Defendants knew the counterparty to the transaction and sought confirmation from it establishes that they were aware of the contract and business expectancy.

C. Defendants Intentionally Interfered.

The third element of tortious interference, intentional interference, speaks to both intent and causation. *Commerce Funding Corp. v. Worldwide Sec. Servs. Corp.*, 249 F.3d 204, 212 (4th Cir. 2001) (applying Virginia law). "The requisite level of intent [for tortious interference] also exists if the interferor knows that the interference is certain or substantially certain to occur as a result of his [or her] actions." *Id.* at 212-13 (citation omitted). No malice is required; knowledge of the business relationship and the intent to disturb it is sufficient. *Chaves v. Johnson*, 335 S.E.2d 97, 102-103 (Va. 1985) (citing Restatement (Second) Torts § 766, cmt. s).

Here, Defendants contacted representatives of California and informed them that they had concerns about the transaction. Ex. 33, 245:19-246:16. Defendants volunteered information about their own customer that was reasonably calculated to cause California to re-think its transaction with Blue Flame. SOF § B; Ex. 42, 85:1-16, 127:22-129:4, 50:20-51:6, 129:7-130:1; Ex. 44,

40:10-21, 63:3-14, 143:4-144:9; Ex. 35, 247:4-252:11. Defendants knew from prior conversations with Gula and Thomas that California's wire transfer was to pay Blue Flame for the purchase of 100 million N95 masks and that Blue Flame would need to immediately make payments to suppliers. *See* SOF §§ C-D. In other words, Defendants knew that, without California's down payment, Blue Flame would not be able to perform under its contract. Defendants' actions, therefore, were "certain or substantially certain" to prevent performance of the contract and result in California breaching the contract, terminating its business relationship with Blue Flame, and/or Blue Flame being unable to perform its obligations under the contract. This is more than sufficient to establish intentional interference. *See, e.g., Commerce Funding Corp.*, 249 F.3d at 213 (finding intentional interference prong was satisfied by a defendant-third party twice contacting plaintiff's contractual counterparty in order to harm performance of plaintiffs' contract or while knowing that such result was substantially certain).

D. Defendants Employed Improper Methods in Interfering.

Where a contract may be terminated at will, and where there was an interference with a business expectancy, there is an additional requirement for tortious interference: the use of "improper methods." *Dunlap*, 754 S.E.2d at 318. Among the most egregious examples of improper methods are those "that are illegal or independently tortious, such *as violations of statutes, regulations, or recognized common-law rules*." *Duggin v. Adams*, 360 S.E.2d 832, 836 (Va. 1987) (emphasis added). Violations of "established standard[s] of a trade or profession" and unethical conduct also constitute improper means. *Id.* at 837.

As demonstrated above, Defendants' actions violated Chain Bridge's obligations under the UCC and Regulation J. That alone establishes improper methods. *See Duggin*, 360 S.E.2d at 836.

Defendants' actions also violated established standards of banking industry practice. Contacting Blue Flame's contractual counterparty to discuss the transaction and divulge

information about Blue Flame and its principals was not consistent with typical banking industry practice. *See, e.g.,* Ex. 42, 97:22-98:6, 98:10-22 (testimony by STO official that "no, it's not typical for us to speak to the counterparty's bank;" it was "unusual" to be contacted by a counterparty's bank; and she could not recall any other instance of the recipient bank speaking with her). Teresa Pesce, JPMC's banking expert witness, testified that she was not aware of an instance where in connection with a BSA investigation (Defendants' proffered justification) executives from a bank directly contacted the counterparty to the transaction, as opposed to the counterparty's bank who originated the wire transfer. Ex. 82, 26:7-28:4; *see also* Ex. 83, 264:12-265:2.

Not only were Defendants actively contacting Blue Flame's contractual counterparty, but they also actively avoided discussing the Wire Transfer with their own client, Blue Flame, once it was received. *See, e.g.*, Ex. 61, CBB00000748; Ex. 26, 226:9-228:22, 243:11-245:7, 267:17-268:11; *see also* Ex. 83, 129:20-130:16, 149:5-153:15 (it is standard industry practice for a bank to request additional information from a customer if there are concerns about a transaction). Indeed, Evinger and Brough never followed up with Gula regarding their purported concerns or requests for further documentation, even after Gula asked if Defendants had any questions. *See* SOF § C; Ex. 37, BFM000013445; Ex. 33, 229:1-17, 230:7-11. Such deviations from typical industry practice constitute improper methods under Virginia law. *See Duggin*, 360 S.E.2d at 837.

CONCLUSION

For the reasons stated herein, Plaintiff respectfully requests this Court to grant partial summary judgment in its favor with respect to liability under Counts I, II, IV, and V, as requested in its Motion for Partial Summary Judgment.

Dated: May 6, 2021

Respectfully submitted,

/s/ *Peter H. White*

Peter H. White (VA Bar No. 32310)
Jason T. Mitchell (*pro hac vice*)
Gregory Ketcham-Colwill (*pro hac vice*)
SCHULTE ROTH & ZABEL LLP
901 Fifteenth Street, NW, Suite 800
Washington, DC 20005
Tel.: (202) 729-7476
Fax: (202) 730-4520
pete.white@srz.com
jason.mitchell@srz.com
gregory.ketcham-colwill@srz.com

William H. Gussman, Jr. (*pro hac vice*)
Steven R. Fisher (*pro hac vice*)
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, New York 10022
Tel.: (212) 756-2044
Fax: (212) 593-5955
bill.gussman@srz.com
steven.fisher@srz.com

Counsel for Plaintiff Blue Flame Medical LLC

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of May, 2021, I caused the foregoing document to be filed and served electronically using the Court's CM/ECF system, which automatically sent a notice of electronic filing to all counsel of record.

Dated: May 6, 2021

/s/ *Peter H. White*

Peter H. White, Esq. (VSB# 32310)
SCHULTE ROTH & ZABEL LLP
901 Fifteenth Street, NW, Suite 800
Washington, DC 20005
Tel: 202-729-7476
Fax: 202-730-4520
peter.white@srz.com

Counsel for Blue Flame Medical LLC